

In The Drawings:

Please amend FIGs. 1-3, as shown in the attached drawings. Replacement FIGs. 1-3 are also submitted herewith, reflecting the changes provided.

### **REMARKS**

FIGs. 1-3 stand objected to because they are not labeled as prior art. In response, Applicants submit amended FIGs. 1-3, which illustrate and label three media used for a digital ticket in embodiments of the present invention. The specification has also been amended to add reference characters where appropriate. The media shown in the labeled Figures are not prior art because, as described in the specification of the present application, a digital ticket according to embodiments of the present invention is stored on each of the media. For example, the disc 12 shown in FIG. 2 is not prior art because, according to the specification, the disc includes a digital ticket stored thereon. Applicants respectfully submit that no new matter is introduced by these drawing amendments. Applicants further request reconsideration and withdrawal of the drawing objection.

Claims 1-30, 38-44, 46, and 48 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. Particularly, the Examiner objects to a number of phrases in claims 1, 8, 23, 24, 29, 30, 38, and 45. Applicants have amended these claims to attempt to address each of the Examiner's objections, and have cancelled claim 46 without prejudice. Applications respectfully request that the indefiniteness rejection has been overcome with respect to each of the claims, and thus Applicants respectfully request reconsideration and withdrawal of the rejection.

Claims 38-46 and 41-55 stand rejected under 35 U.S.C. §102(e) as being anticipated by Mengin. Applicants respectfully traverse the rejection. Regarding claim 38, Mengin fails to teach or suggest at least a ticket buyer's computer comprising means for

determining a number (determined by the ticket buyer only) and means for computing the non-invertible transformation. Though the Office Action cites a “digimas” for such a number and a hashed “digimas” for such a non-invertible transformation, both the “digimas” and the hashed “digimas” are composed by the merchant M, not the buyer’s computer. See, for example, paragraphs 75-77 of Mengin.

As to claim 39, Mengin fails to teach or suggest, in addition to the features described above regarding claim 38, at least the additional feature wherein the communication channel is sending at the second time a random number. The random number cited in the Office Action (paragraph 20 of Mengin) is not a number determined by the ticket buyer only, as is defined in claim 38. Instead, this number would be determined by the ticket seller in Mengin. Accordingly, Applicants respectfully submit that claim 38 and dependent claims 39-44 are allowable over the references of record, including Mengin.

As to claim 45, Mengin fails to teach or suggest at least a printed ticket having a 2-D bar code containing a one-way function of a number provided by a holder of the ticket, where the one-way function is digitally signed by a provider of the ticket. Instead, in Mengin, the one-way function (i.e. the hashed “digimas”) is of a number (“digimas”) provided by the merchant, not a holder of the ticket. Even though the digimas is formed using information from the holder of the ticket, the provider of the ticket provides the number by converting this information into a message, e.g., by concatenating the information in a prescribed, constant order (paragraph 51), and then creating a digital message, or “digimas”. Accordingly, Applicants respectfully submit that claim 45 is allowable over Mengin.

As to claim 51, Mengin fails to disclose or suggest at least the claimed feature of sending from the computer of a ticket buyer to the computer of the ticket seller (not buyer) second data accompanied by a secure first transformation of the number that is determined by the ticket buyer only and unknown to others including the ticket seller. As clearly stated in paragraphs 51-55 of Mengin, a message is concatenated by the merchant, in a prescribed constant order, and it is reinterpreted digitally by the merchant to form the digimas. Because the ticket seller, i.e., the ticket merchant, prepares this number, the number is clearly not determined by the ticket buyer only, and it is clearly known by the merchant. Accordingly, Applicants respectfully submit that claim 51 and dependent claims 52-55 are allowable over the references of record including Mengin.

Claims 8, 24, 30, 32-37, 48, 49 and 50 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Rosen, and with respect to claim 48 unpatentable over Rosen in view of Mengin. Applicants respectfully traverse the rejection for at least the following reasons.

As to claim 8, Rosen fails to teach or suggest at least first calculating in the computer of the consumer a number R, second calculating in the computer of the ticket consumer a one-way function of R as hash(R), transmitting to the ticket provider hash(R), and third calculating in the computer of the ticket provider a digital signature of hash(R) to create Sign(s,I||hash(R)). The Office Action cites col. 12, lines 1-15 for teaching these features, but the hash function and encryption described therein are for certification of a trusted agent or certification of a trusted server. No transaction in the cited portion of Rosen

takes place between a ticket consumer (either a customer or a customer's trusted agent (CTA)) and a ticket buyer (either a merchant or merchant's trusted agent (MTA)). Thus, there is no number R in Rosen that is calculated by a ticket consumer and hashed by the ticket consumer, then transmitted to a ticket provider for digitally signing. By the time the ticket consumer and ticket buyer in Rosen transmit information between one another, the steps cited in the Office Action have already taken place. For at least these reasons, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 8.

As to claim 24, Rosen fails to disclose or suggest at least the claimed features of a ticket consumer's computer that transmits ticket order data to a ticket provider's computer and a ticket provider's computer that receives the first transmitted ticket order data and digitally signs the ticket data. The Office Action cites col. 6, lines 7-12, describing a digital signature of an electronic object, but the digital signature is not from received ticket order data transmitted from the ticket consumer. The Office Action also col. 12, lines 1-3, but this is directed to validating certification of a trusted agent, and does not describe a transaction between a ticket provider's computer and a ticket consumer's computer, nor does it more particularly describe a digital signature from a ticket provider's computer of data provided by a ticket consumer's computer.

Regarding claim 30, Rosen does not disclose or suggest a ticket containing a digital signature comprising a digital representation of  $\text{Sign}(s, I || \text{hash}(R)) || R$ , where R is a random number private to the ticket consumer, where  $\text{hash}(R)$  is a one-way function of R, and where  $\text{Sign}(s, I || \text{hash}(R))$  is a digital signature in respect of signature key s private to the

ticket provider of the hash(R) appended to information I. The Office Action cites cols. 11 and 12. However, cols. 11 or 12 neither disclose nor suggest that a digital signature of the issuer of the ticket (either a merchant or an MTA) is made of hash(R) where R is a random number private to the ticket consumer (consumer or CTA).

Similarly, Applicants respectfully submit that claim 32 is allowable, because Rosen fails to teach or suggest at least  $\text{Sign}(s, I || \text{hash}(R)) || R$ , where R is a random number private to the ticket consumer, where hash(R) is a one-way function of R, and where  $\text{Sign}(s, I || \text{hash}(R))$  is a digital signature in respect of signature key s private to the ticket provider of the hash(R) appended to information I. Applicants further submit that claim 33 is allowable over Rosen, because Rosen fails to teach or suggest at least a tangible transportable data storage medium containing  $\text{Sign}(s, I || \text{hash}(R)) || R$ , where R has its origin in a computer of the ticket consumer, and is appended to  $\text{Sign}(s, I || \text{hash}(R))$ , computed in the ticket provider as a digital signature in respect of a signature key of a number hash(R) appended to I, which number hash(R) was computed in the computer of the ticket consumer.

As to claim 34, Rosen neither teaches nor suggests a digital ticket comprising second-type data including a signed digital representation of a parameter generated in sequence first by the buyer of the ticket as a non-invertible function of a random number, second by the seller of the ticket as a digital signature of the first-time-made non-invertible function, and third by the buyer of the ticket to attach the selfsame random number. Particularly, Rosen does not disclose that the digital signature of the buyer (merchant or MTA) is of a non-invertible function of a random number produced by the buyer of the ticket

(customer or CTA). The Office Action submits that a non-invertible function is represented by  $\text{hash}(X)$  where  $X$  represents a random number. However, as stated above,  $X$  is not a random number, but equals a trusted server ID concatenated with a trusted server public key, further concatenated with expiration data. Accordingly, Applicants respectfully submit that claim 34 and dependent claims 35-37 are allowable over Rosen.

Claim 48 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Mengin in view of Rosen. Applicants respectfully traverse the rejection at least because Rosen fails to teach or suggest the claimed feature of a number  $\text{Sign}(s, I || \text{hash}(R))$ , where  $\text{hash}(R)$  was computed in the computer of the ticket provider as a one-way function of  $R$ , and subsequently communicated to the computer of the ticket provider, and where  $R$ , having its origin in a computer of the ticket consumer, is private to the ticket consumer and is not public. Additionally, Mengin fails to remedy the deficiencies of Rosen because Mengin also fails to teach or suggest at least that  $R$  is a number having its origin in a computer of a consumer of a ticket, and is private to the ticket consumer. Applicants thus respectfully request reconsideration and withdrawal of the rejection.

Regarding claim 49, Applicants respectfully traverse the rejection for at least the reason that Rosen fails to teach or suggest ticket buyer computer at a first time sending at least a one-way transformation of a private number from a ticket buyer computer to a seller computer and a signing at a second time, by the ticket seller computer, this one-way transformation and additional information. The Office Action cites cols. 11 and 12 of Rosen for teaching these features. However, any one-way transformation of a number in these cited

columns is of a number X or Y. Rosen fails to teach or suggest sending a one-way transformation of either X or Y from a ticket buyer computer to a seller computer, nor a signing by the ticket seller computer, of this one-way transformation. Again, X and Y are generated as part of a certification process, and this process is not disclosed in Rosen as being between a buyer computer and a seller computer. Accordingly, Applicants respectfully traverse the rejection.

As to claim 50, Rosen neither teaches nor suggests a sending of a one-way transformation of a private number from a ticket buyer computer to a ticket seller computer, signing at a second time the one-way transformation and additional information in the ticket seller computer, and sending at a second time the one-way transformation and additional information to the ticket seller computer. Instead, the cited portion of Rosen teaches a certification process that does not take place between a buyer and a seller computer. Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection.

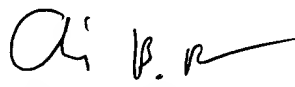
For at least the foregoing reasons, Applicants believe that this case is in condition for allowance, which is respectfully requested. The Examiner should call Applicants' attorney if an interview would expedite prosecution.

Respectfully submitted,  
GREER, BURNS & CRAIN, LTD.

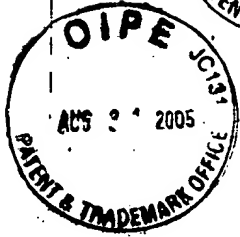
**Customer No. 24978**

August 29, 2005

300 South Wacker Drive  
Suite 2500  
Chicago, Illinois 60606  
Telephone: (312) 360-0080  
Facsimile: (312) 360-9315

By:   
Arik B. Ranson  
Registration No. 43,874





SYSTEM AND METHOD FOR DELIVERING...  
Kobayashi et al.  
Greer Burns & Crain, Ltd.  
Reference No.: 0321.67683  
Annotated FIG. 1

August 29, 2005  
Serial No. 09/490,354  
(Steven P. Fallon)  
(312) 360-0080

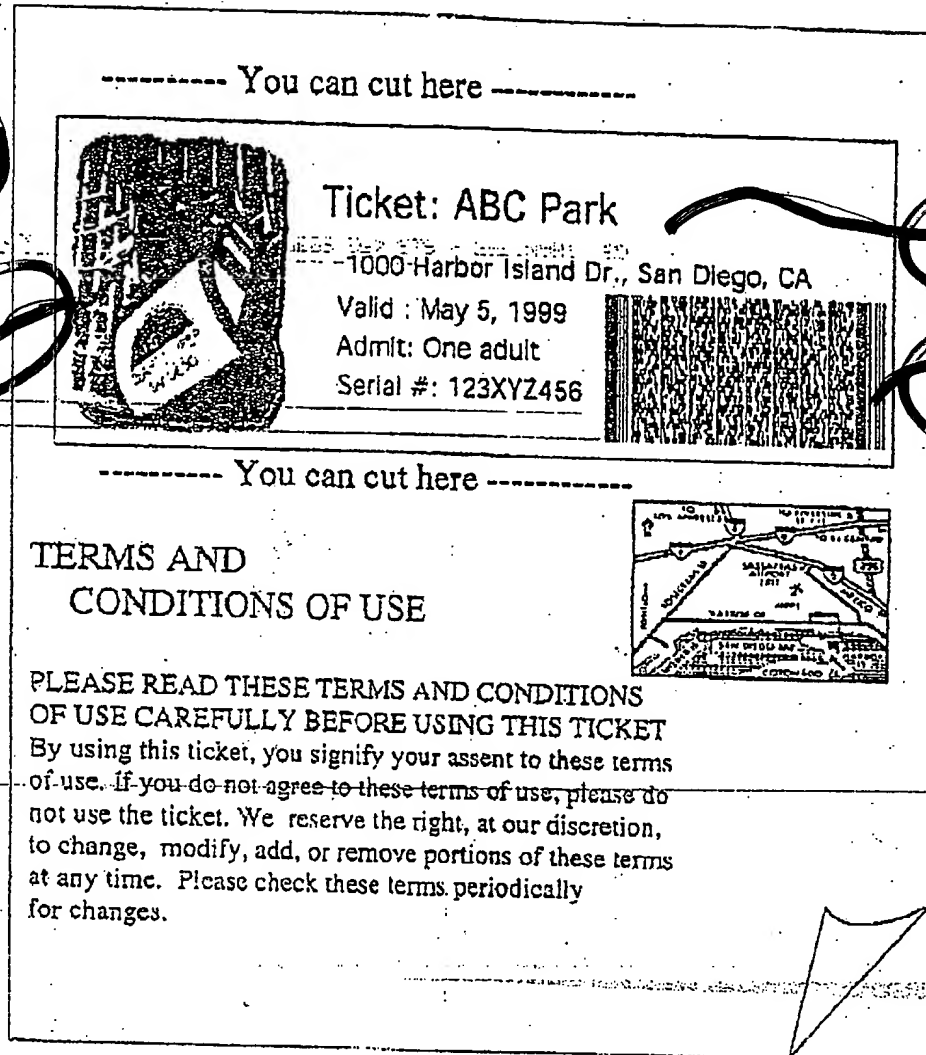


Figure 1: A ticket example.



SYSTEM AND METHOD FOR DELIVERING...  
Kobayashi et al.  
Greer Burns & Crain, Ltd.  
Reference No.:0321.67683  
Annotated FIGs. 2-3

August 29, 2005  
Serial No.09/490,354  
(Steven P. Fallon)  
(312) 360-0080

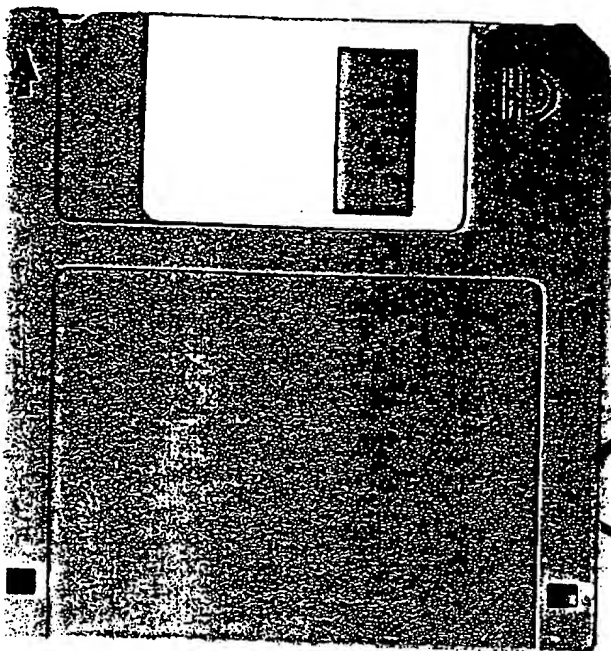


Figure 2

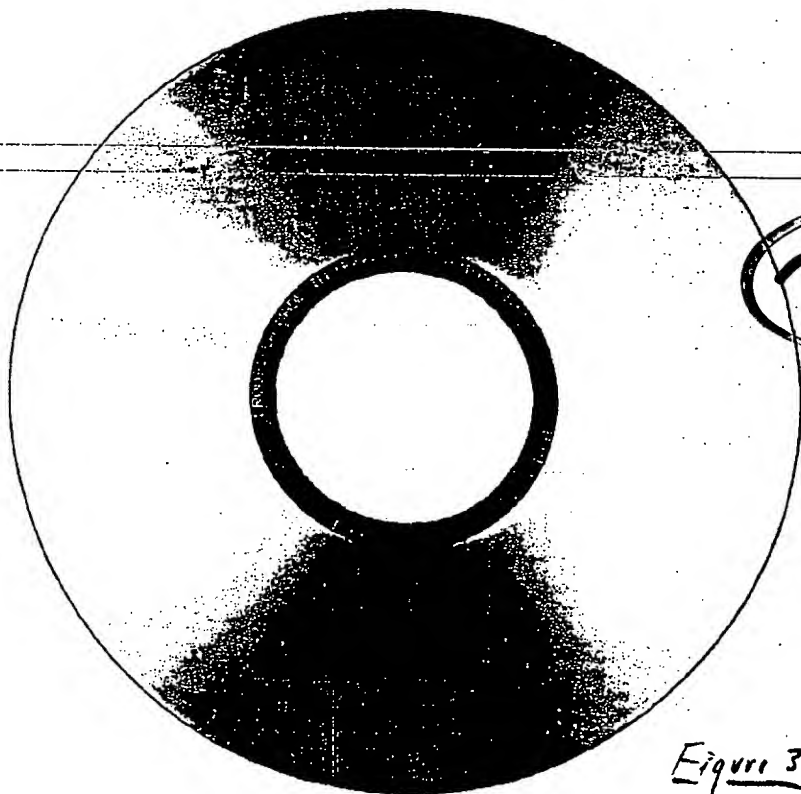


Figure 3

BEST AVAILABLE COPY